The Maritime Executive
INTELLECTUAL CAPITAL FOR LEADERS

Report: Shipping Execs Believe They Are Ready for Cyberattacks

iStock

Published Nov 13, 2024 10:40 PM by The Maritime Executive

Many maritime professionals may have an overoptimistic view of cybersecurity readiness, according to a new study by DNV. More than 60 percent are willing to accept cyber risk in order to pursue digital innovation, and more than 80 percent believe they are ready to defend against hackers - but experts who deal with those incidents every day believe that the maritime industry may be more vulnerable.

In a new survey of nearly 500 staff and executives from shipping companies, offshore operators, shipyards, regulators, ports and vendors, DNV found that the overwhelming majority of participants - eight in 10 - are confident that their company is ready to defend against a cyber incident and respond after the fact. 71 percent expressed confidence that their organization could quickly return to business after an attack. The statistics, however, suggest a different picture.

"The average maritime cyber incident takes 57 days to resolve . . . that's two months," said Daniel Ng, CEO of CyberOwl, a cybersecurity consultancy recently acquired by DNV.

Part of the challenge is that every shipping company is different. The maritime industry is diverse and not highly consolidated, so preparedness varies greatly by organization. Smaller companies are less focused on integrating cybersecurity into all of their assets, says Lim Shih Hsien, Executive Vice President, Cyber IT and OT at Seatrium.

"The largest organizations are very aware of the risk and have strong requirements, such as asking for penetration testing before anything new goes into production – for both IT and OT. But smaller

organizations and individual ship owners are more narrowly focused on the bottom line, avoiding additional new costs," Lim said.

When it comes to the response to a cyberattack, fully 86 percent of respondents said that they known what to do if an incident happens. But preparations depend on accurate and thorough drills, says Wärtsilä's Matti Suominen, and the reality of an actual incident may well be different. Without accurate exercises, a company may not be as ready as its leaders think.

"You may have everything set up to respond to an incident in theory, but the moment you try to collaborate internally – to make sure each team does the right thing let alone all the vendors and other partners – it becomes much harder," Suominen says.

The survey respondents appeared to echo this view: three-quarters said that the current cybersecurity trainings for their staff were not enough to prepare for sophisticated attacks, like AI-enabled phishing.

One of the most consequential areas of cyber-preparedness training is a years-old issue: the use of non-secure USB sticks to transfer files to and from ships. If the process is not well-controlled, it has the potential to spread malicious software.

"Around eight in every 10 [cyberattack] incidents are still delivered via the USB sticks that are necessary for vessel operations," says CyberOwl's Ng. "One of the worst cases we saw recently involved a port where the same USB stick spread malware linked to espionage onto eight vessels. A threat starts on one ship or terminal and can quickly spread across multiple fleets."